2131 0440

Atty. Dkt. No. 043034/0164

#2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Kazue SAKO

Title: ANONYMOUS PARTICIPATION AUTHORITY MANAGEMENT SYSTEM

Appl. No.: 09/765,390

Filing Date: 01/22/2001

Examiner: Unknown

Art Unit: Unknown

CLAIM FOR CONVENTION PRIORITY

Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

- Japanese Patent Application No. 2000-012490 filed 01/21/2000.

Respectfully submitted,

By _____ LYLE KIMMS REG. NO. 34079

Date April 10, 2001

David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

F05-5110US
SAKO
09/765,390

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed this Office.

出願年月日
Date of Application: ２０００年 １月２１日

出願番号
Application Number: 特願２０００－０１２４９０

出願人
Applicant (s): 日本電気株式会社

２０００年１０月１３日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２０００－３０８４３８６

【書類名】　特許願

【整理番号】　33509682

【あて先】　特許庁長官殿

【国際特許分類】　G06F 19/00

【発明者】

【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内

【氏名】　佐古　和恵

【特許出願人】

【識別番号】　000004237

【氏名又は名称】　日本電気株式会社

【代理人】

【識別番号】　100097157

【弁理士】

【氏名又は名称】　桂木　雄二

【手数料の表示】

【予納台帳番号】　024431

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】

匿名参加権限管理システム

【特許請求の範囲】

【請求項１】　管理者サブシステムと、前記管理者サブシステムにより付与された秘密情報を有しこの秘密情報を用いて複数のセッションにまたがって参加できる権限を有する参加者サブシステムと、受付サブシステムからなり、

前記参加者サブシステムが前記秘密情報を用いて複数のセッションにまたがって参加しても検出されない匿名参加が可能である匿名参加権限管理システムであって、

前記参加者サブシステムが、参加するセッションに対して、秘密鍵を用いて参加に伴う個別情報をオーソライズする匿名署名機能を有し、

受付サブシステムが、送付されてきた情報が匿名で参加できる権限を有する参加者サブシステムがオーソライズした匿名署名付きのものであることを検証する匿名署名検証機能と、送付された任意の２つの匿名署名付き情報が、同一の参加者サブシステムが署名したものかどうかを判定する送信元一致判別機能とを有することを特徴とする匿名参加権限管理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は電子アクセス、電子入札、電子抽選、電子嘆願、電子投票などにおいて、複数のセッションにアクセスあるいは参加する権限がある参加者が、自分の名前はおろか、セッション間での参加関係も知られずに匿名で参加できるが、同一のセッション内では同一の参加者が何回参加したか判定できるシステムに関する。

【０００２】

【従来の技術】

従来はブラインド署名を用いた匿名参加方式が検討されていた。ブラインド署名とは、署名する主体が、署名する内容を見ずに署名する方式である。たとえば

、電子投票を行う場合であれば、参加に伴うデータとは自分の投票内容になる。

【０００３】

そこで電子投票は以下のようにして行うことができる。まず、投票権のある参加者サブシステム（申告者）は、自分が投票権があることを管理者サブシステムに証明したあと、投票内容をブラインド署名で署名してもらう。

【０００４】

次に、この管理者サブシステムの署名が付与された投票文を検証サブシステムに送付する。検証サブシステムは送付された投票文に管理者のサブシステムがあるものを、有権者が送付した投票文とみなす。同一の参加者サブシステムが同一の投票セッションに２回以上参加することを防止するために、各投票データには、参加者サブシステム毎に異なるデータを利用することと、管理者サブシステムは各参加者サブシステムに一回しかブラインド署名を発行しないこととする。

【０００５】

これにより、同一の署名つき投票内容が送付されてきた場合には、同一の参加者サブシステムが２度投票しようとしたことと判定できる。ブラインド署名を用いているため、管理者サブシステムであっても、署名つき投票文をどの参加者サブシステムに発行したものかわからないため、匿名性が保たれる。

【０００６】

同様にブラインド署名を用いて、匿名証明書を利用した電子投票方式も検討されている。上述の従来例では、投票に参加するたび、すなわち投票セッション毎に管理者サブシステムにブラインド署名を発行してもらわないといけない。そこで以下では、一度の登録手続きにより、何度も電子投票などに参加できる従来例を紹介する。

【０００７】

まず、参加者サブシステムは、自分が匿名で参加できる権限を有する参加者サブシステムであるということを前記管理者サブシステムに証明した後に、自分の公開鍵をブラインド署名で署名してもらう。この管理者サブシステムの署名が付与された公開鍵を匿名証明書と呼ぶ。

【０００８】

次に、投票内容を自分の秘密鍵で署名し、署名つきの投票内容と、前記匿名証明書を検証サブシステムに送付する。検証サブシステムは送付された匿名証明書に管理者サブシステムの署名が付与された公開鍵であることと、投票文の署名がこの公開鍵に基づき正しく検証できることを確認し、確認できればこれは有権者が送付した投票文とみなす。同一の参加者サブシステムが同一の投票セッションに２回以上参加していないことは、同一の匿名証明書に基づく投票文がないことにより確認する。

【０００９】

ブラインド署名を用いているため、管理者サブシステムであっても、匿名証明書をどの参加者サブシステムに発行したものかわからないため、匿名性が保たれる。ただし、同一の匿名証明書を用いて二つの投票セッションで投票すると同一参加者サブシステムが参加していることがわかってしまう。

【００１０】

次にグループ署名について述べる。これは、同じ匿名証明書を用いて２つ以上の署名を行っても、同一の署名者が署名したものかどうかを秘匿するものである。この技術については、J. Camenischと M. Stadler により、国際会議CRYPTO'97 の中の「Efficient group signature schemes for large groups」という論文に詳しく述べられている。

【００１１】

まず、参加者サブシステムは、自分が匿名で参加できる権限を有するグループに属する参加者サブシステムであるということを前記管理者サブシステムに証明した後に、グループ用秘密鍵を発行してもらう。

【００１２】

次に、送りたいデータをこの秘密鍵で署名し、署名つきのデータを検証サブシステムに送付する。

【００１３】

検証サブシステムは送付されたデータはグループ用公開鍵で検証できるの署名が付与されていることを確認し、確認できればこれは有権グループに属する参加者サブシステムが送付したデータとみなすことができる。グループ署名を用いて

いるため、各署名が、グループ内のどの参加者サブシステムの持つグループ秘密鍵を用いて生成されたのか、区別する手法がないため匿名性が保たれる。

【００１４】

しかしながら、このシステムでは同一の参加者サブシステムが同一のセッションに２回以上データを送付していても、２つの署名が同一のグループ用秘密鍵によって署名されたかどうかを検証する手段がないため、二重投票を防止しなくてはいけない電子投票などには用いることができない。

【００１５】

グループ署名と同様な技術に供託識別という技術があり、この技術はJ. Kilian とE. Petrankにより、国際会議CRYPTO 98 の中の「Identity Escrow 」という論文に詳しく述べられている。しかし、これも同様に２つの識別情報が同一の参加者サブシステムから発行されたものかどうか判定するすべがない。

【００１６】

グループ署名を応用して署名の数が、異なる参加者サブシステムの数に一致するサブグループ署名という技術がある。この技術については、G. Ateniese とG. TsudikJにより、国際会議Financial Cryptography 99 の中の「Some open issues and new directions in group signatures 」という論文に詳しく述べられている。しかし、この場合、全参加者サブシステムで共通のデータに対する署名を施すことになるので、各参加者で送付データの内容が異なる投票には利用することができない。

【００１７】

【発明が解決しようとする課題】

上述したように従来の技術には、電子投票や電子入札に利用できるように、一度の登録処理で複数のセッションに参加でき、且つ同一の参加者からのデータが存在した場合には特定でき、さらに複数のセッションにまたがって参加しても検出されずセッション間の参加関係は秘匿できる方式というのは存在していなかった。

【００１８】

先に説明した様に、ブラインド署名によって送付データを署名する従来技術に

おいては各セッション毎に登録処理を行う必要があり、匿名証明書を用いる従来技術はセッション間の参加関係が秘匿できず、グループ署名や供託識別は同一参加者によるセッションの参加が検証できず、またサブグループ署名を用いるものでは各参加者サブシステムが独立に参加データを作成することができなかった。

【００１９】

そこで、本発明では上述した実状に鑑み、電子投票や電子入札に利用すべく、一度の登録処理で複数のセッションに参加でき、且つ同一のセッションでは同一の参加者が複数回参加したことが判明できるが、セッション間の参加関係は秘匿できる匿名参加権限管理システムシステムを新たに提案することを目的とする。

【００２０】

【課題を解決するための手段】

本発明による匿名参加権限管理システムは、管理者サブシステムと、前記管理者サブシステムにより付与された秘密情報を有しこの秘密情報を用いて複数のセッションにまたがって参加できる権限を有する参加者サブシステムと、受付サブシステムからなり、前記参加者サブシステムが前記秘密情報を用いて複数のセッションにまたがって参加しても検出されない匿名参加が可能である匿名参加権限管理システムであって、前記参加者サブシステムが、参加するセッションに対して、秘密鍵を用いて参加に伴う個別情報をオーソライズする匿名署名機能を有し、受付サブシステムが、送付されてきた情報が匿名で参加できる権限を有する参加者サブシステムがオーソライズした匿名署名付きのものであることを検証する匿名署名検証機能と、送付された任意の２つの匿名署名付き情報が、同一の参加者サブシステムが署名したものかどうかを判定する送信元一致判別機能とを有することを特徴とする。

【００２１】

【発明の実施の形態】

以下本発明の目的、特徴および利点を明確にすべく、本発明の実施の形態を挙げ添付した図面を参照しながら詳細に説明する。本発明の一実施の形態としてのシステムを図１～図３により示す。図１は参加者サブシステム101 を、図２は受付サブシステム102 をそれぞれ示している。また、図３はシステムの概念図を示

す。

【００２２】

例えば、本匿名参加権限管理システムを電子投票の投票者管理システムに適用するとすると、参加者サブシステムは投票者サブシステムであり、投票権のある各投票者は事前に管理者サブシステムから秘密情報を付与されており、受付サブシステムは投票受付を行う。

【００２３】

セッションは各選挙事象（国勢選挙、地方自治体選挙など）であり、セッションに関連するセッション関連情報は選挙セッションを特定する情報を含みすべて、あるいは一定の範囲の投票者（たとえば同一の選挙管理地域の投票者）に共通の情報であり、個人データとは各投票者で異なる投票データである。

【００２４】

また、「匿名署名」というのは、従来の署名者が特定される「デジタル署名」と異なり、署名者名は特定されずに匿名であるが、その匿名の参加権限を持つ人が確かに作成し、他人によって改竄されていないことを署名のように保証（オーソライズ）することを示す。なお、デジタル署名方式によっては、署名対象のデータが署名データから明白に分離されるものと、署名データに間接的に署名対象のデータが含まれるものの２通りがある。そこで、ここで述べる匿名署名、あるいは匿名署名が付与された参加データとは、匿名署名対象のデータが含まれることとする。

【００２５】

図１および２を参照すると、本参加者サブシステム101 は、事前に管理者サブシステム100 と交信して付与された秘密情報10を秘密情報保持手段20に持ち、参加したいセッションのセッション関連情報11と、参加したいセッションへの入力となる個人データ12を前記秘密鍵保持手段20で保持する秘密鍵10を用いて匿名署名機能21にてオーソライズした匿名参加データ13を生成し、これを受付サブシステム102 に匿名で送付する。

【００２６】

受付サブシステム102 はこの参加データを受け取り、これが該セッションに匿

名で参加できる権限を有する参加者サブシステムがオーソライズした個人データを含むものであることを匿名署名検証手段30にて検証する。

【００２７】

次に受理済参加データの各データが、送付された参加データと同一の参加者サブシステムが送付したものではないかどうかを判定する送信元一致判別手段31により参加者が以前に参加しているかどうかを判定する。

【００２８】

投票の場合ならば、以前に参加していなければ、該送付された参加データを受理し、以前に参加があればこれを受理して通知する。

【００２９】

あるいは、すべての検証済データをまず受付しておき、受付済参加データの中で同一の参加者サブシステムがないと送信元一致判別手段31により確認できたものを受理してもよい。

【００３０】

入札など他の場合は、最初の参加に伴うデータのみを受理したり、あるいは最新の参加データを有効にしたり、あるいは同一参加者サブシステムの参加データのうち、ある基準でひとつだけ選択し有効にすることもできる。もちろん、匿名署名検証手段を用いた参加データの検証も、受信後の任意の時に行えばよい。

【００３１】

また、例えば本匿名参加権限管理システムを電子入札の入札者管理システムに適用すると、参加者サブシステムは入札者サブシステムであり、入札資格のある各入札者は事前に管理者サブシステムから秘密情報を付与されており、受付サブシステムは入札受付を行う。

【００３２】

セッションは各入札案件であり、セッションに関連するセッション関連情報は入札セッションを特定する情報を含みすべての入札者に共通の情報であり、個人データとは各入札者で異なる入札データである。

【００３３】

例えば、本匿名参加権限管理システムを電子抽選の応募者管理システムに適用

した場合には、参加者サブシステムは応募者サブシステムであり、応募資格のある各応募者は事前に管理者サブシステムから秘密情報を付与されており、受付サブシステムは応募受付を行う。

【００３４】

セッションは各抽選案件であり、セッションに関連するセッション関連情報は抽選セッションを特定する情報を含みすべての応募者に共通の情報であり、個人データとは各応募者で異なる応募データである。

【００３５】

以下、本実施の形態の動作につき説明する。具体例としてグループ署名を応用した例について述べる（図４参照）。

【００３６】

グループ署名として、J. CamenischとM. Stadlerが、国際会議CRYPTO'97 の中の「Efficient group signature schemes for large groups」という論文で紹介した方式が知られている。

【００３７】

上記の文献に記載されているように、n をRSA 暗号で用いられているような２素数の積とし、g を、位数n の巡回群を生成する生成元とし、a を、n と互いに素な整数とし、e を、n のオイラー数と互いに素な整数とし、δを、１以外の定数とした共通定数(g,a,e,n, δ）が必要になる。

【００３８】

そこで、管理者システム100 はこれらの共通定数を生成し、n の素因数を管理者システムの秘密情報とする。これらの生成方法は上記文献に詳しく論じられている。

【００３９】

各参加者サブシステム101 は、n の素因数を知っている管理者システムと交信することにより、前記共通定数(g,a,e,n, δ）に対して

$$v=(y+\delta)^{(1/e)} \bmod n$$

を満たす秘密情報10(x,y,v) を入手する。ここでy=a ^ x mod n である。

【００４０】

ここで、秘密情報(x,y,v) の入手方法は、管理者システムがすべてを生成して参加者サブシステムに配布してもいいし、各参加者サブシステムがx を秘密にして、y のみを提出し、管理者システムにy からv を算出してもらってもよい。また、ブラインド署名技術を用いて、y さえも見せずに秘密情報(x,y,v) を入手することもできる。

【００４１】

次に以下で用いる証明方式について先に紹介する。

【００４２】

SKREP(y,g)[(α): y=g^(α) }](m)

とは、y=g ^(α) を満たすαを知っていることを(y,g,m) を用いて証明することである。ここでm は任意の数である。

【００４３】

SKLOGLOG(y,g,a)[(α): y=g^(a^ α) }](m)

とは、y=g ^(a^ α) を満たすαを知っていることを(y,g,a,m) を用いて証明することである。ここでm は任意の数である。

【００４４】

つぎに、

SKROOTLOG(y,g,e)[α: y=g ^(α^e)](m)

とは、y=g ^(α^e)を満たすαを知っていることを(y,g,e,m) を用いて証明することである。ここでm は任意の数である。

【００４５】

具体的な証明文の生成方法および証明文の検証方法は上記の文献に詳しく、また本発明に直接関係しないので、ここでは触れない。

【００４６】

次に、セッション管理情報A(11) 、個人データm(12) を用いた匿名署名機能21として、図４に示すような下記の演算を行う。

【００４７】

まず、生成元作成手段52にて、セッションA に対応した生成元gAを入手し、次にgmをgm=Hash(m)により生成する。

【００４８】

次に、グループ署名手段51にてz=gA＾y とし、z=gA＾(a＾α) となるαを知っていることを証明する証明文V1=SKLOGLOG(z,gA,a)[(α): z=gA ＾(a＾α)](1)を生成し、 z*gA ＾δ=gA ＾(β ＾e)となるβを知っていること証明する証明文V2=SKROOTLOG(z*gA ＾δ,gA,e)[β: z*gA＾δ=gA ＾(β ＾e)](1)を生成する。

【００４９】

なお、ここでSKLOGLOG，SKROOTLOG の入力となる定数1 は、セッション関連情報として与えられ、外部データ入力手段50からの出力となる定数である。

【００５０】

次に関連付けデータ生成手段53手段にてz=gA＾y とし、z1とz はそれぞれgA,gm をベースにして同じ巾であることを証明する証明文V3=SKREP(z1/z, gm/gA)SKREP[γ:z1/z= (gm/gA)＾γ](1)を作成する。

【００５１】

上記の処理の出力として、参加データ13を(A,m,z,z1,V1,V2,V3) とする。なお、A が明らかな場合はAを敢えて参加データに加える必要はない。

【００５２】

また、生成元作成手段52において、gAはセッション関連情報の一部として与えられてもよいし、あるいはgA=Hash(A)として生成してもよい。

【００５３】

この参加データ13を受信した受付サブシステムは、A からgAを入手し、匿名署名検証手段30にて証明文V1,V2,V3がそれぞれ正しいことを確認する。

【００５４】

次に送信元一致判別手段31においては、参加データ中で同じz がある場合には、これらの参加データは同一の参加者サブシステムが送付したものであると判定できる。これは、同じ参加者サブシステムからの参加データに含まれるz は個人データm の値に関わらず同一セッションに対して同じであるからである。

【００５５】

以上のようにすれば、同一の秘密情報10(x,y,v) を用いて異なるセッションに参加してもその関連が判明しないが（なぜならば、異なるベースに対して同じ巾

で巾乗した数とそうでないものの区別は難しいからである。）同一のセッションに参加した場合はその関連が判明する匿名参加権限管理システムが構築できる。また、発行した匿名参加用秘密情報を無効にする方式も上記文献で議論されている。

【００５６】

また、当業者にとって、上記の方式のバリエーションを考えることは容易である。たとえば、生成元作成手段52にてgmをgm=Hash(A ||m)によって生成しても効果はかわらない。ここで||は連結をしめす。さらにはgAやgmはそれぞれA やm,あるいはA やA とm により一意的にきまる有限体上の生成元であれば、ハッシュ関数を用いなくてもよい。また、V1,V2,V3を生成する上で、外部データ入力手段50の出力として定数(1) を例として用いたが、これは事前に合意されていれば任意の数でも、gA,gm,y,z 等の変数でもよい。

【００５７】

さらには、生成元作成手段52におけるgmとgAの使い方を変えることもできる。たとえば生成元作成手段52として、個別データm によりgm=Hash(m)により生成し、次にgAをセッション関連情報A を用いてgA=Hash(A)により生成し、次にグループ署名手段51にてz2=gm ^ y とし、z2=gm ^ (a ^ α) となるαを知っていることを証明する証明文V1=SKLOGLOG(z2,gm,a)[(α): z2=gm ^ (a ^ α)] (1) を生成し、z2*gm ^ δ=gm ^ (β ^ e)となるβを知っていること証明する証明文V2=SKROOTLOG(z2*gm ^ δ,gm,e)[β: z2*gm ^ δ=gm ^ (β ^ e)](1)を生成し、関連付けデータ生成手段52にてz3=gA ^ y とし、z2とz3はそれぞれgm,gA をベースにして同じ巾であることを証明する証明文V3=SKREP(z2/z3, gm/gA)SKREP[γ:z2/z3= (gm/gA) ^ γ](1)を作成し、参加データ13を(A,m,z2,z3,V1,V2,V3)としても効果はかわらない。

【００５８】

このとき、送信元一致判別手段31は参加データ中のz3に重複がないかどうか調べることとなる。

【００５９】

また、更に効率を追求した例も考えられる。次に、セッション管理情報A 、個

人データm を用いた匿名署名機能21を図５の参加者サブシステム101Aを参照しながら説明する。

【００６０】

まず、生成元作成手段52にて、セッションA に対応した生成元gAを入手する。次に、外部データ入力手段62からの出力をmとし、グループ署名手段61にてz=gA ^ y とし、z=gA ^ (a ^ α) となるαを知っていることを証明する証明文V1=SKLOG LOG(z,gA,a)[(α):z=gA ^ (a ^ α)](m) を生成し、z*gA ^ δ=gA ^ (β ^ e)となるβを知っていること証明する証明文V2=SKROOTLOG(z*gA ^ δ,gA,e)[β: z*gA ^ δ=gA ^ (β ^ e)](m)を生成し、参加データ13を(A,m,z,V1,V2) とする。なお、A が明らかな場合はA を敢えて参加データに加える必要はない。また、gAはAとともに与えられてもよいし、あるいはgA=Hash(A)として生成してもよい。

【００６１】

この場合、参加データの長さが短くなるだけではなく、匿名署名検証手段30にて証明文V1,V2 のみの正当性を検証すればよく、効率があがる。さらに、外部データ入力手段62からの出力は個人データのみに依存させなくても、セッション管理情報A を含めても検証時に同様に含めれば問題ない。

【００６２】

また、別の供託識別システムに基づかせることもできる。供託識別手法は、J. KilianとE. Petrankが、国際会議CRYPTO 98 の中の「Identity Escrow 」という論文に詳しく述べられている。

【００６３】

本例では上記と同様にn をRSA 暗号で用いられているような２素数の積とし、g を、位数n の巡回群を生成する生成元とし、e を、n のオイラー数と互いに素な整数とし、δを、１以外の定数とした共通定数(g,a,e,n, δ) が必要になる。そこで、管理者システムはこれらの共通定数を生成し、n の素因数を管理者システムの秘密情報とする。

【００６４】

各参加者サブシステムは、n の素因数を知っている管理者システムと交信することにより、前記共通定数(g,e,n, δ) に対してb=(a ^ e-δ) ^ (1/e) mod n を

満たす秘密情報10(a,b) を入手する。

【００６５】

ここで、秘密情報(a,b) を入手方法は、管理者システムがすべてを生成して参加者サブシステムに配布してもいいし、ブラインド署名技術を用いて、a さえも見せずに秘密情報(a,b) を入手することもできる。

【００６６】

次例では、セッション管理情報A 、個人データm を用いた匿名署名機能21として、図６に示すように参加者サブシステム101Bにおいて下記の演算を行う。

【００６７】

まず、生成元作成手段52にて、セッションA に対応した生成元gAを入手し、次にgmをgm=Hash(m)により生成する。

【００６８】

次に、供託識別手段81においてza=gA ^ {a ^ e } とし、za=gA ^(α ^e)となるαを知っていることを証明する証明文V1=SKROOTLOG(za,gA,e)[(α): za=gA ^(α ^e)](1)を生成し、zb=gA ^ {b ^e } とし、zb=gA ^(β ^e)となるβを知っていることを証明する証明文V2=SKROOTLOG(zb,gA,e)[(β): zb=gA ^(β ^e)](1)を生成する。

【００６９】

次に関連付けデータ生成手段53にてzc=gm ^(a ^e)とし、zaとzcはそれぞれgA,gm をベースにして同じ巾であることを証明する証明文V3=SKREP(zc/za, gm/gA) SKREP[γ:zc/za= (gm/gA) ^ γ](1)を作成し、参加データ13を(A,m,za,zb,zc,V1,V2,V3) とする。なお、A が明らかな場合はA を敢えて参加データに加える必要はない。また、gAはセッション管理情報の一部として与えられてもよいし、あるいはgA=Hash(A)として生成してもよい。

【００７０】

この参加データ13を受信した受付サブシステムは、A からgAを入手し、匿名署名検証手段30にてza*zb=gA ^ δ が満たされていることと、証明文V1,V2,V3がそれぞれ正しいことを確認する。

【００７１】

さらに、次に送信元一致判別手段31においては、参加データ中で同じzaがある場合には、これらの参加データは同一の参加者サブシステムが送付したものであると判定できる。これは、同じ参加者サブシステムからの参加データに含まれるzaは個人データm の値に関わらず同一セッションに対して同じであるからである。

【００７２】

また、送信元一致判別手段31において、zaのかわりにzbを検出しても同様の効果がある。

【００７３】

以上のようにすれば、同一の秘密情報10(a,b) を用いて異なるセッションに参加してもその関連が判明しないが（なぜならば、異なるベースに対して同じ巾で巾乗した数とそうでないものの区別は難しいからである。）同一のセッションに参加した場合はその関連が判明する匿名参加権限管理システムが構築できる。また、前述の例と異なり、SKLOGLOGより効率のよいSKROOTLOG のみを使っている点で効率がよくなっている。

【００７４】

また、発行した匿名参加用秘密情報を無効にする方式も上記文献で議論されている。

【００７５】

また、当業者にとって、上記の方式のバリエーションを考えることは容易である。たとえば、生成元作成手段52にてgmをgm=Hash(A ||m)によって生成しても効果はかわらない。ここで||は連結をしめす。さらにはgAやgmはそれぞれA やm,あるいはA やA とm により一意的にきまる有限体上の生成元であれば、ハッシュ関数を用いなくてもよい。また、V1,V2,V3を生成する上で、外部データ入力手段50の出力として定数(1) を例として用いたが、これは事前に合意されていれば任意の数でも、gA,gm,y,z 等の変数でもよい。

【００７６】

さらには、生成元作成手段52おけるgmとgAの使い方を変えることもできる。たとえば生成元作成手段52において、gAをセッション関連情報A を用いてgA=Hash(

A)により生成し、個別データmによりgm=Hash(m)により生成し、次に供託識別手段81にてza=gm ^ {a ^ e } とし、za=gm ^ (α ^ e)となるαを知っていることを証明する証明文V1=SKROOTLOG(za,gm,e)[(α): za=gm ^ (α ^ e)](1)を生成し、zb=gm ^ {b ^ e } とし、zb=gm ^ (β ^ e)となるβを知っていることを証明する証明文V2=SKROOTLOG(zb,gm,e)[(β): zb=gm ^ (β ^ e)](1)を生成する。

【００７７】

次に関連付けデータ生成手段53にてzc=gA ^ (a ^ e)とし、zaとzcはそれぞれgm,gA をベースにして同じ巾であることを証明する証明文V3=SKREP(zc/za, gA/gm) SKREP[γ:zc/za= (gA/gm) ^ γ](1)を作成し、参加データ13を(A,m,za,zb,zc,V1,V2,V3) としても効果はかわらない。

【００７８】

このとき、送信元一致判別手段31は参加データ中のzcに重複がないかどうか調べることとなる。

【００７９】

また、更に効率を追求した例も考えられる。次に、セッション管理情報A 、個人データm を用いた匿名署名機能21を図７の参加者サブシステム101Cを参照しながら説明する。

【００８０】

まず、生成元作成手段60にてセッションA に対応した生成元gAを入手する。

【００８１】

次に、外部データ入力手段62からの出力をm とし、供託識別手段91にてz=gA ^ y とし、za=gA ^ {a ^ e } とし、za=gA ^ (α ^ e)となるαを知っていることを証明する証明文V1=SKROOTLOG(za,gA,e)[(α): za=gA ^ (α ^ e)](m)を生成し、zb=gA ^ {b ^ e } とし、zb=gA ^ (β ^ e)となるβを知っていることを証明する証明文V2=SKROOTLOG(zb,gA,e)[(β): zb=gA ^ (β ^ e)](m)を生成し、参加データ13を(A,m,za,zb,V1,V2) とする。なお、A が明らかな場合はA を敢えて参加データに加える必要はない。また、gAはA とともに与えられてもよいし、あるいはgA=Hash(A)として生成してもよい。

【００８２】

この場合、参加データの長さが短くなるだけではなく、匿名署名検証手段30にて証明文V1,V2 のみの正当性を検証すればよく、効率があがる。

【００８３】

本例のもうひとつのメリットは、匿名署名検証手段や送信元一致判別手段において、受付システム固有の秘密情報が不要である点である。したがって、電子投票の正当性を検証するために、参加データをすべて公開すれば、すべての参加データが正当な有権者の投票であり、なおかつ同一の有権者であっても二重投票を行っていないことを誰でも検証できる。また、このようなシステムは電子嘆願書にも応用できる。

【００８４】

電子入札においては、受付システムが特定の参加者サブシステムから複数の参加データ（入札データ）を受け付けておき、後でその中で最も優位なデータを残すという不正が考えられ、この場合は誰もが送信元一致判別手段を利用できても、この不正は検出できない。その場合は、開封前に（すなわち優位なデータがどれか判明する前に）受け付けた参加データを特定し、それから変更できないようにしたり、あるいは、受け付けた参加データに対する領収書を、以前の参加データに依存させる形で発行することにより、参加データを削除した場合は他の参加者の持っている領収書と不一致が生じて、不正が発覚する。

【００８５】

なお、本例においては、一般の数体の上の演算として紹介したが、たとえば楕円曲線上の演算として読み替えたり、他の群、あるいは体の上の演算として読み替えても同様な効果が得られることは当業者にとって明らかである。

【００８６】

なお、本発明が上記各実施例に限定されず、本発明の技術思想の範囲内において、各実施例は適宜変更され得ることは明らかである。

【００８７】

【発明の効果】

以上説明したように、本願発明によれば、電子投票や電子入札に利用可能なように、参加者サブシステムは管理者サブシステムとの一度の登録処理で複数のセ

ッションに匿名で参加でき、さらにセッション間の参加関係は秘匿でき、受付サブシステムは参加データが参加権限のある参加者サブシステムが送付したデータであることを検証でき、さらに、同一の参加者サブシステムからの参加データが存在した場合には特定できるという匿名参加権限管理システムが提供される。

【図面の簡単な説明】

【図１】本発明における参加者サブシステムの実施の形態の構成を示すブロック図である。

【図２】本発明における受付サブシステムの実施の形態の構成を示すブロック図である。

【図３】本発明システム実施の形態の構成を示すブロック図である。

【図４】本発明における匿名署名機能の実施の形態の構成を示す参加者サブシステムのブロック図である。

【図５】本発明における匿名署名機能の実施の形態の構成を示す参加者サブシステムのブロック図である。

【図６】本発明における匿名署名機能の他の実施の形態の構成を示す参加者サブシステムのブロック図である。

【図７】本発明における匿名署名機能の更に他の実施の形態の構成を示す参加者サブシステムのブロック図である。

【符号の説明】

20…秘密鍵保持手段

21…匿名署名機能

22…送信機能

30…匿名署名検証手段

31…送信元一致判別手段

33…受信機能

50…外部データ入力手段

51…グループ署名手段

52…生成元作成手段

53…関連付けデータ生成手段

60…生成元作成手段

61…グループ署名手段

62…外部データ入力手段

81…供託識別手段

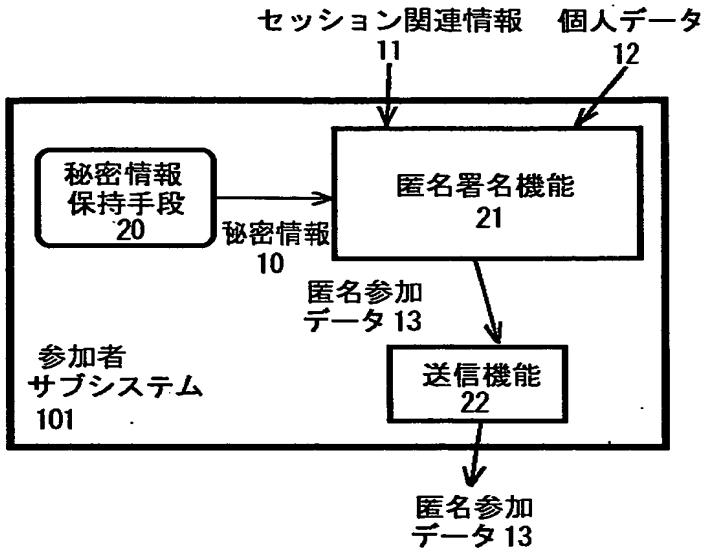
100 …管理者サブシステム

101,101A,101B,101C…参加者サブシステム

102 …受付サブシステム

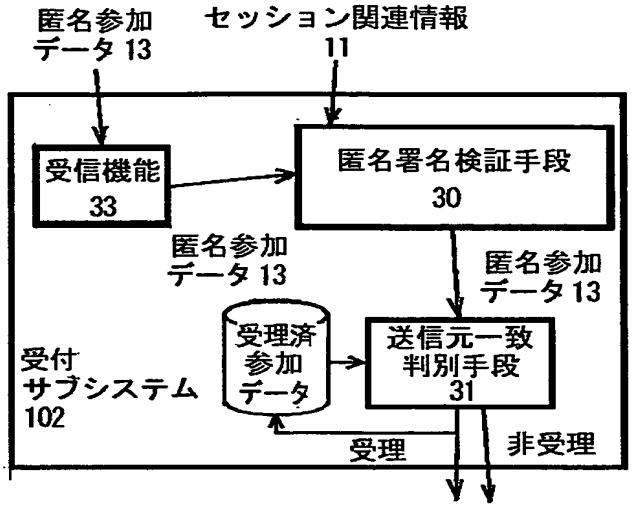
【書類名】　　図面

【図１】

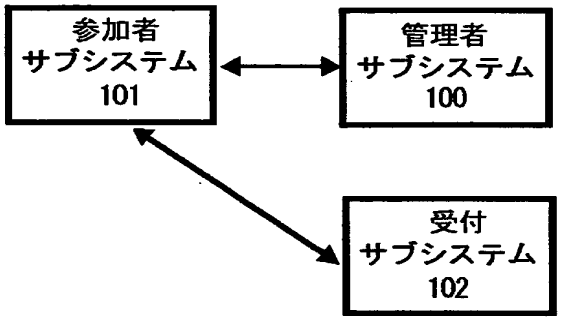


出証特２０００－３０８４３８６

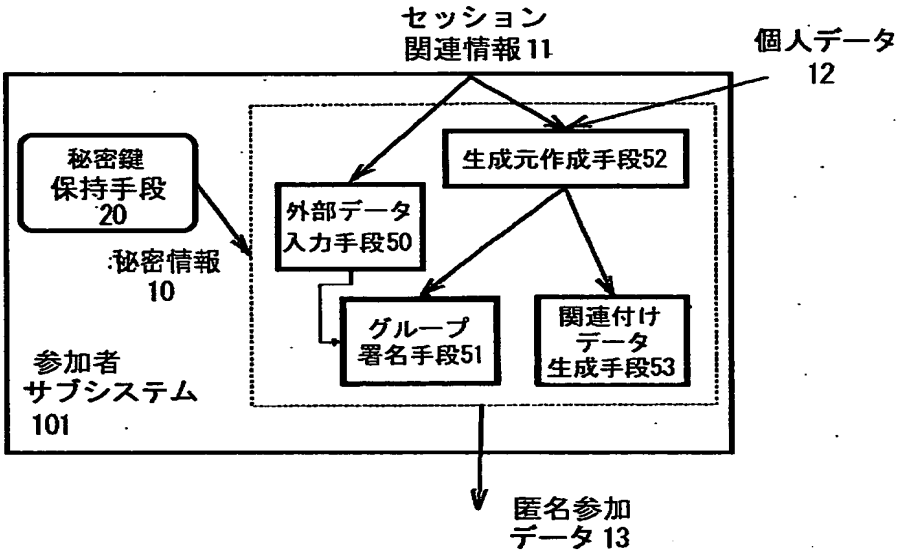
【図２】


匿名参加
データ 13
セッション関連情報
11
受信機能
33
匿名署名検証手段
30
匿名参加
データ 13
匿名参加
データ 13
受理済
参加
データ
送信元一致
判別手段
31
受付
サブシステム
102
受理
非受理

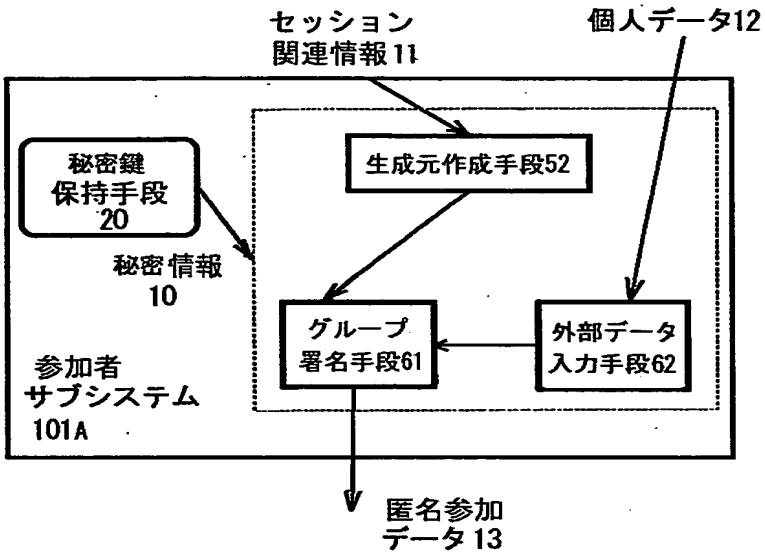
【図３】



【図４】

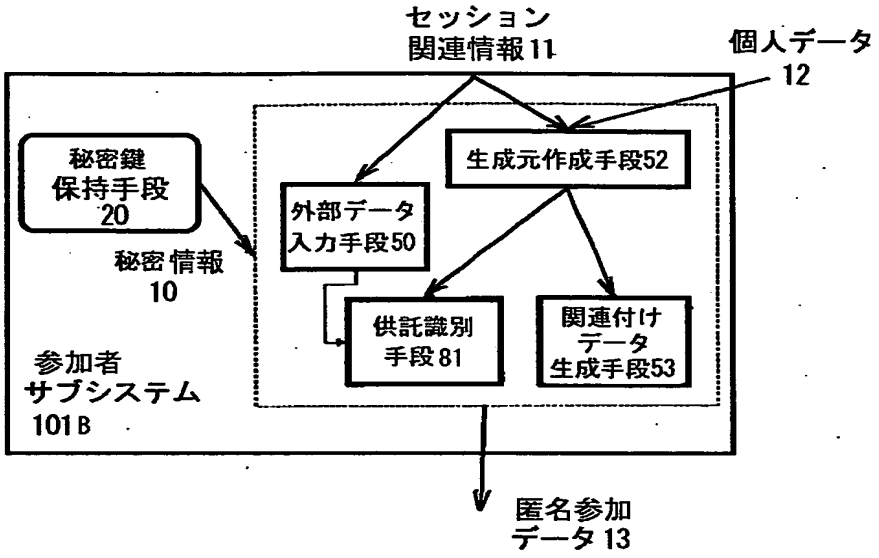

セッション
関連情報11
個人データ
12
秘密鍵
保持手段
20
秘密情報
10
外部データ
入力手段50
生成元作成手段52
グループ
署名手段51
関連付け
データ
生成手段53
参加者
サブシステム
101
匿名参加
データ13

【図５】

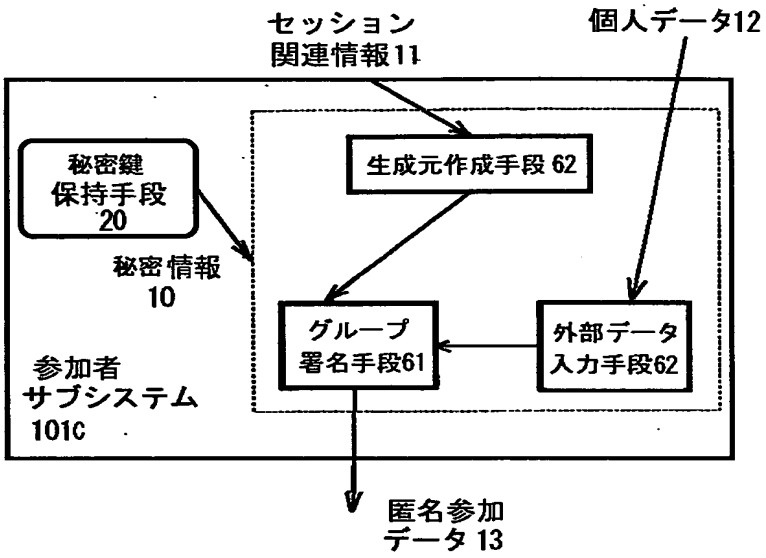


出証特２０００－３０８４３８６

【図６】


セッション
関連情報11
個人データ
12
秘密鍵
保持手段
20
秘密情報
10
外部データ
入力手段50
生成元作成手段52
供託識別
手段81
関連付け
データ
生成手段53
参加者
サブシステム
101B
匿名参加
データ13

【図７】


セッション
関連情報11
個人データ12
秘密鍵
保持手段
20
生成元作成手段 62
秘密情報
10
グループ
署名手段61
外部データ
入力手段62
参加者
サブシステム
101c
匿名参加
データ 13

【書類名】　　要約書

【要約】

【課題】参加者サブシステムが前記秘密情報を用いて複数のセッションにまたがって参加しても検出されずに匿名参加が可能であり、重複参加を検出・防止可能で、匿名参加権限管理システム参加者の申告値を秘匿しながら、当選者の申告値の正当性を保証する当選者判定システム等の匿名参加権限管理システムを提供する。

【解決手段】管理者サブシステムと、前記管理者サブシステムにより付与された秘密情報を有しこの秘密情報を用いて複数のセッションにまたがって参加できる権限を有する参加者サブシステムと、受付サブシステムからなり、前記参加者サブシステムが、参加するセッションに対して、前記秘密鍵を用いて参加に伴う個別情報をオーソライズする匿名署名機能を有し、受付サブシステムが、送付されてきた情報が匿名で参加できる権限を有する参加者サブシステムがオーソライズした匿名署名付きのものであることを検証する匿名署名検証手段と、２つの匿名署名付き情報が、同一の参加者サブシステムが署名したものかどうかを判定する送信元一致判別手段とを具備して匿名参加権限管理システムを構成する。参加者サブシステムにおける暗号化機能の部分に、申告値に依存した暗号パラメータを供給し、このパラメータに依存して暗号化を行う。復号は、当選値の復号パラメータで順に暗号データを復号し、無事に復号できたものがそのパラメータに対応する申告値であったと判定でき、当選値以外の申告値に関する情報を秘匿することができる。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２０００－０１２４９０
受付番号	５００００５８１９２
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１２年　１月２４日

＜認定情報・付加情報＞

【提出日】　平成12年 1月21日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００４２３７〕

１．変更年月日　　１９９０年　８月２９日
［変更理由］　新規登録
住　所　東京都港区芝五丁目７番１号
氏　名　日本電気株式会社